(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－10930
（P2000－10930A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.⁷		識別記号	F I			テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｄ	５Ｂ０８５
	13/00	３５１		13/00	３５１Ｚ	５Ｂ０８９
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ	５Ｋ０１３
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ	
					６７５Ｄ	

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－177017

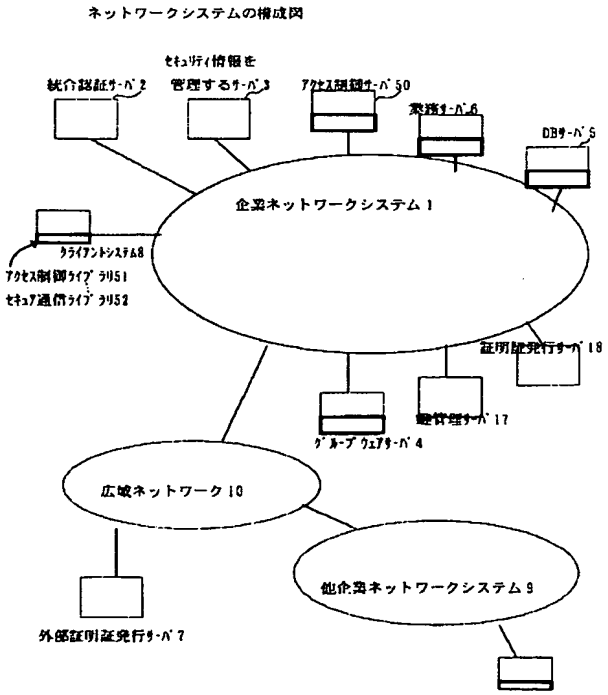
(22)出願日　平成10年６月24日(1998.6.24)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　齊藤　洋子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

Ｆターム(参考)　5B085 AE02 AE06 AE10 AE23
5B089 AA21 AA22 AC05 AE08 AE09
AF00 CB02 CB03 CE00 DD03
DD07 EA03
5K013 AA08 FA01 GA05

(54)【発明の名称】　ネットワークシステムでのアクセス制御方法

(57)【要約】
【課題】業務サーバ，ＤＢサーバ，グループウェアサーバ等が従来のＡＣＬで行っていたアクセス制御処理を、アクセス制御サーバで集中的に一元管理する。またアクセスチケットを利用して、ネットワークシステム利用の一時的制約やユーザのアクセス状況を把握して、より柔軟なネットワーク運用を行う。
【解決手段】ユーザの認証後あるいはクライアント８，２０からアクセス制御サーバ５０に対してユーザの業務要求が転送された時に、アクセス制御サーバ５０が統合認証サーバ２によるユーザの証明証の確認結果からユーザの業務サーバ６へのアクセス権限のチェックを行い、正当であれば業務サーバ６へのユーザの業務要求を許可する。その場合、通信内容を第三者には見せないことを保証する。



【特許請求の範囲】
【請求項１】　ユーザが共有するクライアント端末，該クライアントからアクセスされ、業務処理のために利用される業務サーバ、および該ユーザが各サーバにアクセスする権限を有するか否かを確認するアクセス制御サーバが、相互に通信可能なネットワークシステムでのアクセス制御方法において、
ユーザを認証した後、あるいは該ユーザが共有するクライアント端末から該アクセス制御サーバに対して該ユーザの業務要求が転送された時に、
該アクセス制御サーバが、該ユーザの証明証の確認結果から該ユーザの業務サーバへのアクセス権限をチェックするステップと、
該アクセス制御サーバは、該アクセス権限が正当であれば該業務サーバへのユーザの業務要求を許可するステップとを有することを特徴とするネットワークでのアクセス制御方法。
【請求項２】　ユーザが共有するクライアント端末にアクセス制御ライブラリを設け、ユーザが各サーバにアクセスする権限を有するか否かを確認するアクセス制御サーバのＩＤ，該ユーザのＩＤ，アクセス制御リスト、運用の制約条件、該アクセス制御サーバの署名情報等から構成されるアクセスチケット情報を利用して、ユーザのアクセス権限のチェックを行うネットワークシステムでのアクセス制御方法において、
該アクセス制御サーバで、前記アクセスチケット情報を作成し、該アクセスチケット情報を該アクセス制御ライブラリに送信するステップと、
該アクセス制御ライブラリで、該アクセスチケット情報を用いて該ユーザの業務サーバへのアクセス権限チェックを行い、該業務サーバへのアクセス要求が適切であった場合には、該業務サーバに該ユーザの業務要求と該アクセスチケット情報を転送するステップと、
該業務サーバで、該ユーザによるデータへのアクセス権限のチェック結果を含むアクセス履歴情報を作成し、該ユーザによるアクセスの終了時に、業務結果と前記アクセス履歴情報を付加したアクセスチケット情報を該アクセス制御ライブラリに送信するステップと、
該アクセス制御ライブラリで、該アクセスチケット情報の内容を確認し、該ユーザのアクセス状況をチェックし、該アクセス状況に問題があった場合には、セキュリティ侵害情報を作成して、該セキュリティ侵害情報を付加したアクセスチケット情報を該アクセス制御サーバに送信するステップとを有することを特徴とするネットワークシステムでのアクセス制御方法。
【請求項３】　請求項１または２に記載のネットワークシステムでのアクセス制御方法において、
前記アクセス制御サーバ、クライアント端末のアクセス制御ライブラリ、及び業務サーバとの間でアクセスチケット情報を送受信する際に、通信の当事者以外には該アクセスチケット情報の内容を見せないよう保証することを特徴とするネットワークシステムでのアクセス制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、認証サーバ、アクセス制御サーバ、およびクライアントに対して、証明証を利用して広域ネットワークシステムでユーザ認証およびアクセス制御を行うネットワークシステムでのアクセス制御方法に関する。
【０００２】
【従来の技術】インターネットの普及に伴いセキュリティをめぐる市場動向はめざましく変化してきた。特に、インターネットとイントラネットを統合する認証サーバは重要であり、広域ネットワークシステムでユーザを一元管理し、さらに集中的にアクセス制御を行う機能が求められている。ユーザ認証及びアクセス制御に証明証を利用する方法は、今後の広域ネットワークシステムでは一般的になると思われる。しかし、現実のネットワークシステムを考えると、最初から一元的なユーザ管理を行うことは困難であり、従来のユーザのネットワークシステムや業務形態に応じて、各業務サーバが個別にユーザのアクセス制御を行うことになると考えられる。この様なシステムの問題点としては、例えば企業内の人事移動に伴う職制変更等の時などに、複数の業務システムのデータベースのユーザ情報（例えば、認証情報やアクセス制御情報）を変更しなければならない点である。
【０００３】本出願人は、本願より先に２つの提案（特願平９－７６９５４号（先願Ａ）、および特願平９－１７３５３２号（先願Ｂ）の各明細書および図面参照）を行っているが、先願Ａでは、統合認証サーバで証明証によりユーザを認証することにより、従来のパスワードによる認証処理とのシングルサインオンを実現している。また、クライアントと統合認証サーバの双方でユーザに関するアクセス履歴を取得し、両者を比較することによりユーザの不正なアクセス状況をチェックしている。一方、先願Ｂでは、このセキュリティ管理モデルを拡張し、ユーザが複数の証明書により取り引きを行う場合に証明書の管理を容易化している。具体的には、統合認証サーバで１枚の統合証明書によりユーザを認証し、クライアントから業務APあるいは通信相手への通信要求に応じて、取り引きに必要な証明書を通信の当事者に送信するようにしている。先願Ｂの方式は、統合認証サーバで統合証明書の確認を集中的に行うシステム形態を想定しており、この場合には前記通信要求に関するユーザのアクセス権限の確認を統合証明書の認証処理の延長で行うことができる。なお、本願では、先願Ａに合わせて認証サーバが発行する証明を証明証と記載する。
【０００４】
【発明が解決しようとする課題】前述のように、統合認

証サーバで統合証明証の確認を集中的に行うシステム形態のアクセス制御方式については、先願Ｂに開示されている。しかしながら、認証処理のために統合認証サーバを設けず、通信の当事者間で、例えばセキュア通信ライブラリを実装することにより認証プロトコルに基づいて相互認証するシステム形態を考えると、アクセス制御を集中的に管理するアクセス制御サーバを設けたセキュリティ管理の方が適していると考える。

【０００５】そこで、本発明の目的は、このような従来の課題を解決し、前記セキュア通信ライブラリと連携してアクセス制御を実現することにより、企業内のネットワークシステムを１箇所から集中管理することが可能なネットワークシステムでのアクセス制御方法を提供することにある。また、本発明の他の目的は、アクセス制御ライブラリを通信の当事者に実装したシステム形態を考慮し、その場合に必要となる前記アクセス制御サーバとの間のアクセス権限情報を送受信することができる機能を有するネットワークシステムでのアクセス制御方法を提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明によるネットワークシステムでのアクセス制御方法では、①ユーザを認証した後に、あるいは該ユーザが共有するクライアントからアクセス制御サーバに対してユーザの業務要求が転送された時に、アクセス制御サーバが該ユーザの証明証の確認結果からユーザの該業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへのユーザの業務要求を許可することを特徴とする。また、本発明のアクセス制御方法では、㊤クライアントにアクセス制御ライブラリを設ける場合には、アクセス制御サーバＩＤ，ユーザＩＤ，アクセス制御リスト、制約条件、署名情報等から構成されるアクセスチケット情報を利用して、ユーザのアクセス権限をチェックするために、次の処理を行うことも特徴とする。(1)アクセス制御ライブラリで、前記アクセスチケットを用いて該ユーザの業務サーバへのアクセス権限チェックするステップと、該業務サーバへのアクセス要求が適切であった場合には該業務サーバに該ユーザの業務要求と前記アクセスチケットを転送するステップと、(2)業務サーバで、該ユーザによるデータへのアクセス権限のチェック結果を含むアクセス履歴情報を作成するステップと、該ユーザによるアクセスの終了時に業務結果と前記アクセス履歴情報を付加したアクセスチケットを該アクセス制御ライブラリに送信するステップと、(3)該アクセス制御ライブラリで、前記アクセスチケットの内容を確認して該ユーザのアクセス状況をチェックするステップと、該アクセス状況に問題があった場合にはセキュリティ侵害情報を作成するステップと、前記セキュリティ侵害を付加したアクセスチケットを該アクセス制御サーバに送信するステップとを有することである。

【０００７】さらに、本発明のアクセス制御方法では、㊤アクセス制御サーバ、クライアントのアクセス制御ライブラリ及び業務サーバとの間で送受信されるアクセスチケットの情報については、通信の当事者以外には見せないことを保証することも特徴とする。本発明では、証明証を基にユーザのアクセス制御情報を参照することにより、全てのサーバへのアクセス制御を行う方式を提案する。すなわち、証明証を利用して広域ネットワークシステムでユーザ認証及びアクセス制御を行う認証サーバとアクセス制御サーバに関わるものであり、先願Ａで提案した統合認証サーバとの連携を実現するアクセス制御方法を対象としている。これにより、業務サーバやデータベース（ＤＢ）サーバ、グループウェアサーバ等が、従来ではＡＣＬ（アクセス制御リスト）で行っていたアクセス制御処理を、アクセス制御サーバで集中的に一元管理することができ、またアクセスチケットを利用することにより、ネットワークシステム利用の一時的制約やユーザのアクセス状況を把握することができ、柔軟なネットワークの運用が可能になる。

【０００８】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明が適用されるネットワークシステムの構成図である。インターネットのような広域ネットワーク１０には、企業ネットワークシステム１と他企業ネットワークシステム９が接続される。企業ネットワークシステム１には、複数のクライアント８（ここでは、１個のみ示されている）の他に、統合認証サーバ２，セキュリティ情報を管理するサーバ３、アクセス制御サーバ５０、業務サーバ６、ＤＢサーバ５、グループウェアサーバ４，鍵管理サーバ１７，および証明証発行サーバ１８等の各サーバが接続される。ここで、ＤＢサーバ５および業務サーバ６は、クライアント８からアクセスされ、かつ業務処理のために利用されるサーバである。また、グループウェアサーバ４は、クライアント８へ最初の業務メニュー画面を送ったり、クライアント８の電子メールの送受信管理をしたり、ユーザのスケジュールを管理したりするサーバである。一方、他企業ネットワークシステム９には、クライアント２０が接続されており、クライアント８のユーザとクライアント２０は、電子取り引き等の特定の業務を証明証を用いて行うものとする。なお、クライアントシステム８には、アクセス制御ライブラリ５１とセキュア通信ライブラリ５２が備えられ、これを黒枠で示しており、ネットワークシステム１，９に接続されているクライアントシステム２０と各サーバ４，５，６，５０にも同じライブラリが備えられていることを黒枠で示している。

【０００９】セキュリティ情報を管理するサーバ３は、ＤＢサーバ５および業務サーバ６または他企業ネットワークシステム９へのアクセスを制御する情報と、業務に

キュリティ情報とを、一元的に管理するサーバである。公開鍵等もこのサーバ３で扱われる。また、統合認証サーバ２は、クライアント８から送られる証明証を確認し、サーバ３からセキュリティ情報を取得してユーザが企業ネットワークシステム１にログインする資格を持つか否かを調べる。このユーザの識別と認証処理が終了すると、ユーザのＤＢサーバ５および業務サーバ６または他企業ネットワークシステム９へのアクセス権限をチェックする必要があるため、該ユーザのＡＣＬ（アクセス制御リスト）をサーバ３に要求する。該ＡＣＬの要求処理は、統合認証サーバ２がユーザの認証処理の延長で行うことにより、サーバ３から取得したセキュリティ情報の中からＡＣＬだけをアクセス制御サーバ５０に渡すように実装することも可能であり、また、アクセス制御サーバ５０が直接前記サーバ３からＡＣＬを取得するように実装することも可能である。また、ＡＣＬを取得するタイミングとしては、ユーザの認証処理の後でも、ユーザからの業務要求を受けた時でもよい。

【００１０】図２は、本発明におけるＡＣＬを取得する手順および業務要求に対して許可／拒絶を受ける手順を示すシーケンスチャートである。図２（ａ）のシーケンスチャートでは、セキュア通信ライブラリ５２がユーザを認証した後に、アクセス制御サーバ５０にユーザのアクセス無限の確認要求を行い、アクセス制御サーバ５０がサーバ３にＡＣＬを要求する処理例を示している。また、図２（ｂ）のシーケンスチャートでは、クライアント８のユーザの業務要求がアクセス制御サーバ５０に転送された時に、同時にユーザのアクセス権限の確認要求が行われ、アクセス制御サーバ５０で該ユーザの証明証の確認結果からユーザの該業務サーバへのアクセス権限のチェックを行っている。いずれにしても、アクセス制御サーバ５０は、サーバ３から取得したＡＣＬ情報を用いて、ユーザがＤＢサーバ５および業務サーバ６または他企業ネットワークシステム９にアクセスする権限を持つかどうかを確認するサーバである。また、鍵管理サーバ１７は、企業ネットワークシステム１内での暗号化通信で使用する通信当事者の鍵(秘密鍵と公開鍵の対)を生成するサーバである。広域ネットワーク１０には、外部証明書発行サーバ７が接続されている。この外部証明書発行サーバ７は、所定の手順に従って外部証明書を発行するサーバである。例えば、クライアントシステム８とクライアントシステム２０が広域ネットワーク１０を介して取引を行う場合には、証明証発行サーバ１８あるいは外部証明証発行サーバ７のいずれかに証明証あるいは外部証明証の発行を申請すればよい。

【００１１】なお、ディレクトリサーバ（図示省略：各アプリケーションの存在場所を管理するサーバ）と呼ばれるサーバを配置して、ここにサーバ３の情報を有していても良い。この場合、クライアント８および各種サーバは、パソコン、ワークステーションを含む情報処理装置である。さらに、クライアント８および各種サーバによって各々読み取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して、以下に記述するクライアント８および各種サーバの処理を行うことができる。例えば、アクセス制御ライブラリ５１は、クライアント８上のコンピュータプログラムであり、アクセス制御サーバ５０や業務サーバ６などと通信することにより、ユーザのアクセス状況を監視する。また、セキュア通信ライブラリ５２は、クライアント８上や各種サーバ上のコンピュータプログラムであり、ネットワークシステム内の通信をセキュアに保護するために、通信当事者の相互認証、通信データの暗号化と内容の保証を行う。クライアント８または他企業ネットワークシステム９に接続されるクライアント２０から証明証の情報を入力して、例えばＤＢサーバ５にログインすると、統合認証サーバ２が証明証の確認を行うが、この証明証を用いた具体的な認証処理シーケンスやシングルサインオンの実現方法については、前述の先願発明Ａを参照すれば明らかとなる。

【００１２】図２（ａ）には、ユーザがクライアント８からログイン後にセキュア通信ライブラリ５２、アクセス制御ライブラリ５１、アクセス制御サーバ５０およびサーバ３間でやり取りする処理シーケンスが示されている。ユーザ１１は、クライアント８の表示するユーザ認証画面（１１ａ）にＩＣカード内の証明証３０の情報を入力することにより（１１ｂ）、企業ネットワークシステム１にログインする。ユーザの認証処理については、通信する双方のセキュア通信ライブラリ５２がＩＣカード内のユーザ１１の証明証３０の情報を確認し、乱数情報を送受信するチャレンジレスポンスシーケンスにより相互を認証しあい、そのセションで利用する暗号鍵をネゴシェーションする処理を行うが、本発明では詳細の説明は省略する。具体的な認証シーケンスについては、先願発明Ｂを参照することで明らかとなる。証明証３０の情報を利用してセキュア通信ライブラリ５２の処理によりユーザ１１の正当性が認められた後は、クライアント８上のアクセス制御ライブラリ５１が証明証３０の情報を用いて、ユーザ１１のアクセス権限を確認する。図２（ａ）に示すように、アクセス制御ライブラリ５２は、アクセス制御サーバ５０に対して証明証３０の情報を送信する（１１ｃ）。これにより、アクセス制御サーバ５０は、証明証３０の情報を基にサーバ３に格納されているユーザ１１のアクセス制御リスト(ＡＣＬ)７０を入手要求する（１１ｄ，１１ｅ）。

【００１３】例えば、サーバ３がＬＤＡＰ(Lightweight Data Access Protocol)に基づくディレクトリサーバである場合には、アクセス制御サーバ５０はＬＤＡＰのプロトコルに基づきサーバ３に情報の問合せを行う。ＬＤＡＰのプロトコル処理の一例については、先願発明Ａを参照すれば明らかとなる。そして、ＡＣＬ７０の内容を

確認することにより、アクセス制御サーバ５０は、ユーザ１１の企業ネットワークシステム１へのアクセス権限が確認できる。具体的には、アクセス制御サーバ５０から送信されてきたＡＣＬ７０の情報をもとに、クライアント８側のアクセス制御ライブラリ５１がユーザ１１向けの初期選択画面を表示し（１１ｇ）、以降、ユーザ１１への業務処理サービスを行う（１１ｈ）。なお、アクセス制御サーバ５０とアクセス制御ライブラリ５１との間の通信はセキュア通信ライブラリ５２の機能により保護されているため、相互で正しく認証され、情報が盗まれたり改ざんされたりする心配はない。該セキュア通信ライブラリ５２の処理内容については、先願発明Ａを参照されたい。

【００１４】一方、図２（ｂ）では、クライアント８のユーザの業務要求がアクセス制御サーバ５０に転送された時に、アクセス制御サーバ５０で該ユーザの証明証の確認結果からユーザの該業務サーバへのアクセス権限のチェックを行っている。例えば、ＥＣ向けアプリケーションのように、商品の購入時に初めて認証処理を行う時等に相当する。クライアント８から業務要求を受けた時に（１０ａ）、セキュア通信ライブラリ５２はユーザ認証画面を表示し（１０ｂ）、ユーザはユーザ認証画面にＩＣカード内の証明証３０の情報を入力する（１０ｃ）。証明証３０の情報を利用してセキュア通信ライブラリ５２の処理によりユーザ１１の正当性が認められた後は、クライアント８上のアクセス制御ライブラリ５１が証明証３０の情報を用いて、ユーザ１１のアクセス権限を確認する。図２（ｂ）に示すように、アクセス制御ライブラリ５２は、アクセス制御サーバ５０に対して証明証３０の情報を送信する（１０ｄ）。その結果、アクセス制御サーバ５０は証明証３０の情報を基に、サーバ３に格納されているユーザ１１のアクセス制御リスト（ＡＣＬ）７０を入手要求する（１０ｅ）。そして、ＡＣＬ７０の内容を確認することにより（ＡＣＬ７０ｅ）、アクセス制御サーバ５０は、ユーザ１１の企業ネットワークシステム１へのアクセス権限が確認できる。具体的には、アクセス制御サーバ５０から送信されてきたＡＣＬ７０の情報（ＡＣＬ７０ｆ）を基に、クライアント８側のアクセス制御ライブラリ５１がユーザ１１の業務要求の許可あるいは拒絶を応答する（１０ｇ）。

【００１５】図３は、本発明に用いられるＡＣＬ形式の情報例を示す図である。ＡＣＬには種々の形式が考えられるが、ユーザ情報の更新時に修正作業を最小限にするために、図３（ａ）に示すようにユーザ情報７１とユーザ権限情報７２、およびアクセス関連情報７３をツリー構造の別データとして管理している。ユーザ情報７１には、図３（ｂ）に示すように企業内ネットワーク１内で当ユーザを一意的に識別するために付与されているユーザ識別名称と証明証の情報の対応が管理されている。このユーザ識別名称については、企業システムの名称ポリシーの規定に従う。また、図３（ｃ）に示すようにユーザに関するその他の情報(例えば住所、家族構成や入社年度等の情報)も必要に応じて参照できるようになっている。ユーザ権限情報７２には、図３（ｄ）に示すようにユーザとユーザの権限の対応が管理されている。例えばユーザをＡ０，Ａ１，Ａ２，Ａ３という権限クラスで分類してアクセスさせるようなシステムの場合は、事例１に示すようにユーザごとに権限クラスを指定しておく。また、このようなクラスの代りに、事例２（図３（ｅ））に示すように所属や職位からなる職制情報を利用してもよい。

【００１６】これらの権限クラスや職制情報に対応させて、どのような権限を許可するかを規定しておくのが、図３（ｆ）に示すようなアクセス関連情報７３である。アクセス関連情報７３には、企業ネットワークシステム１内の全リソースに関するアクセス権限情報が定義されているので、例えば、図３（ｆ）に示すように、クラスＡ１のユーザ１１についての企業ネットワークシステム１内のアクセス権限が、ＤＢサーバ５のファイル５０１に対する参照と更新、ファイル５０２に対する参照が許可され、業務サーバ６のＡＰ６０１の起動が許可されていることがわかる。また、接続形態の条件として、企業ネットワーク内からのアクセスだけが許可されており、リモートアクセスによる接続は許可されていないことがわかる。このようにして、全てのユーザに対するアクセス制御情報を一元管理するが、よりきめ細かなアクセス制御、例えばファイル５０３のレコード５０３１（いずれも図示省略）をユーザ１１だけに見せるというアクセスを制御したい場合には、ＤＢサーバ５内のアクセス制御機能を利用することも可能である。職制変更時のユーザ情報変更作業を考えると、例えば、ユーザ１１の担当業務が変更になった場合には、図３（ｅ）に示すユーザ権限情報７２を変更すればよく、ユーザ１１のアカウントが削除される場合には、図３（ｂ）～（ｅ）に示すユーザ情報７１とユーザ権限情報７２からユーザ１１の項目を削除すればよい。従来方式において、業務サーバ毎にユーザのＡＣＬを管理していたシステム形態では、ユーザ情報の修正が業務サーバ毎に必要であったことを考えると、本発明では、ユーザ情報を一個所で変更できる点に利点がある。

【００１７】図４は、本発明におけるアクセスチケットを用いた制御手順を示すシーケンスチャートである。アクセス制御サーバ５０がアクセスチケット７５を用いて、さらにきめ細かな運用を考慮したアクセス制御を行う事例について説明する。図４に示すように、セキュア通信ライブラリ５２はユーザ認証画面を表示し（１４ａ）、ユーザはユーザ認証画面にＩＣカード内の証明証３１の情報を入力する（１４ｂ）。証明証３１の情報を利用してセキュア通信ライブラリ５２の処理によりユーザ１１の正当性が認められた後は、クライアント８上

のアクセス制御ライブラリ５１が証明証３１の情報を用いて、ユーザ１４のアクセス権限を確認する。次に、アクセス制御サーバ５０に対してユーザ１４のアクセス権限の確認要求を行うと（１４ｃ）、アクセス制御サーバ５０は業務サーバ6にＡＣＬを要求する（１４ｄ）。このように、ユーザ１４がクライアント２０からネットワークシステム１にログインする場合、アクセスチケット７５ａの中に9時から１７時までという一時的な運用の制約条件７６をつけることが可能である。この場合、アクセス制御サーバ５０は、クライアント２０側のアクセス制御ライブラリ５１に、アクセス制御サーバＩＤ，ユーザ１４のユーザ識別名、ユーザ１４のＡＣＬ,制約条件７６、およびアクセス制御サーバ５０の署名情報から構成されるアクセスチケット７５ａを作成し、アクセス制御ライブラリ５１に送信する（７５ａ）。アクセス制御サーバ５０とアクセス制御ライブラリ５１との間の通信はセキュア通信ライブラリ５２の機能により保護されているため、相互で正しく認証され、情報が盗まれたり改ざんされる心配はない。また、セキュア通信ライブラリ５１は、アクセスチケット７５ａの内容が確かにアクセス制御サーバ５０によって作成されたものであることを保証するために、署名情報を付加している。

【００１８】次に、図４において、アクセス制御ライブラリ５１がアクセスチケット７５ａを受け取ると、クライアント２０上のグループウェアアプリケーションはユーザ１４に対して初期選択画面を表示する（１４ｅ）。この初期選択画面は、ユーザ１４のＡＣＬに基づき作成されるもので、ユーザ１４に権限に許されている業務だけが表示される。また、ユーザ１４が表示された以外の業務のアプリケーションを起動するとユーザ１４に対して警告を発し、アクセス履歴情報報１２が取得される。ユーザ１４が前記初期選択画面の中の業務の中から業務サーバ6のＡＰ６０（図示省略）を起動した場合（１４ｆ）、ユーザ１４によるＡＰ６０１（図示省略）の業務要求は、アクセス制御ライブラリ５１から業務サーバ6に転送されるが（７５ｄ）、その時に前記アクセスチケット７５ａも添付される。業務サーバ6は、このアクセスチケット７５ａの内容を確認することにより、以降の業務処理ＡＰ６０１を実行する。具体的には、ＡＣＬと制約条件７６を考慮した処理を行うので、図４に示すＡＣＬに許可された以外のＡＰ６０１の修正や業務ＡＰ６０２の起動等は許さず、時刻が１７時を過ぎたならばユーザ１４に対する処理を打ち切る。そして、業務サーバ6は、ユーザ１４のアクセス状況についてはアクセス履歴情報１２に記録しておく。

【００１９】業務が終了すると、業務サーバ6は、業務サーバＩＤ，ユーザ１４のユーザ識別名、ユーザ１４によるアクセス履歴情報１２、および業務サーバ6の署名情報から構成されるアクセスチケット７５ｂを作成し、アクセス制御ライブラリ５１に送信する（７５ｅ）。なお、業務サーバ6とアクセス制御ライブラリ５１との間の通信はセキュア通信ライブラリ５２の機能により保護されているため、相互で正しく認証され、情報が盗まれたり改ざんされたりする心配はない。アクセス制御ライブラリ５１は、ユーザ１４に業務結果を出力するとともに（１４ｇ）、業務サーバ6から受信したアクセスチケット７５ｂのアクセス履歴情報１２を確認し、ユーザ１４のアクセスに問題があるかどうかをチェックし、セキュリティ上の問題を発見した場合には、セキュリティ侵害情報１３とアクセス制御ライブラリ51の署名情報を作成してアクセスチケット７５ｃに付加して送信することにより（７５ｃ）、アクセス制御サーバ５０に報告する。また、図４の例では、制約条件７６をアクセス制御サーバ５０が付加したが、例えば、ユーザのＩＣカードの中にオペレーション情報を格納しておき、その情報を図４のアクセス制御ライブラリ５１によるユーザ１４のアクセス権限の確認要求の時にアクセス制御サーバ５０に送るような実装も可能である。

【００２０】

【発明の効果】以上述べたように、本発明によれば、業務サーバ、ＤＢサーバ、あるいはグループウェアサーバ等が従来のＡＣＬで行っていたアクセス制御処理を、アクセス制御サーバにより一元管理できるので、企業内ネットワークシステムを一個所から集中管理することが可能である。また、アクセスチケットを利用することにより、ネットワークシステム利用の一時的制約やユーザのアクセス状況を把握できるので、より柔軟なネットワーク運用が可能となる。さらに、前記アクセスチケットの情報は、クライアント、業務サーバ、アクセス制御サーバの間でセキュアに送受信されるため、悪意のある第三者が盗聴して悪用することは不可能となる。

【図面の簡単な説明】

【図１】本発明が適用されるネットワークシステムの構成図である。

【図２】本発明におけるＡＣＬ問い合わせ手順および業務要求手順の各シーケンスチャートである。

【図３】本発明で用いられるＡＣＬ形式の情報例を示す図である。

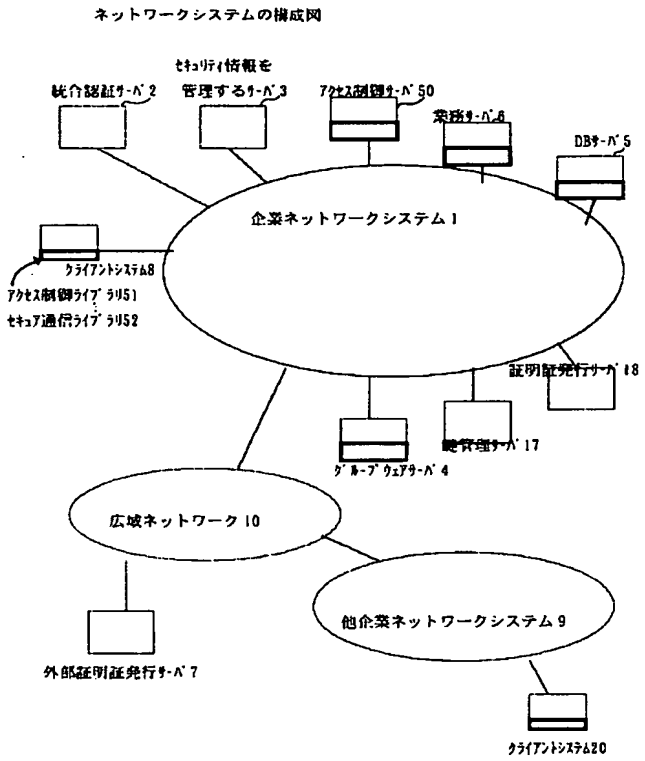
【図４】本発明におけるアクセスチケットを用いた制御手順のシーケンスチャートである。

【符号の説明】

１…企業ネットワークシステム、２…統合認証サーバ、３…セキュリティ情報を管理するサーバ、４…グループウェアサーバ、５…ＤＢサーバ、６…業務サーバ、７…外部証明証発行サーバ、８，２０…クライアントシステム、９…他企業のネットワークシステム、１０…広域ネットワークシステム、１１，１４…ユーザ、１２…アクセス履歴情報、１３…セキュリティ侵害情報、１７…鍵管理サーバ、１８…証明証発行サーバ、３０，３１…証

クセスチケット、７６…制約条件、５１…アクセス制御ライブラリ、５２…セキュア通信ライブラリ、７１…ユーザ情報、７２…ユーザ権限情報、７３…アクセス関連情報、５０…アクセス制御サーバ、Ａ０～Ａ３…権限クラス。

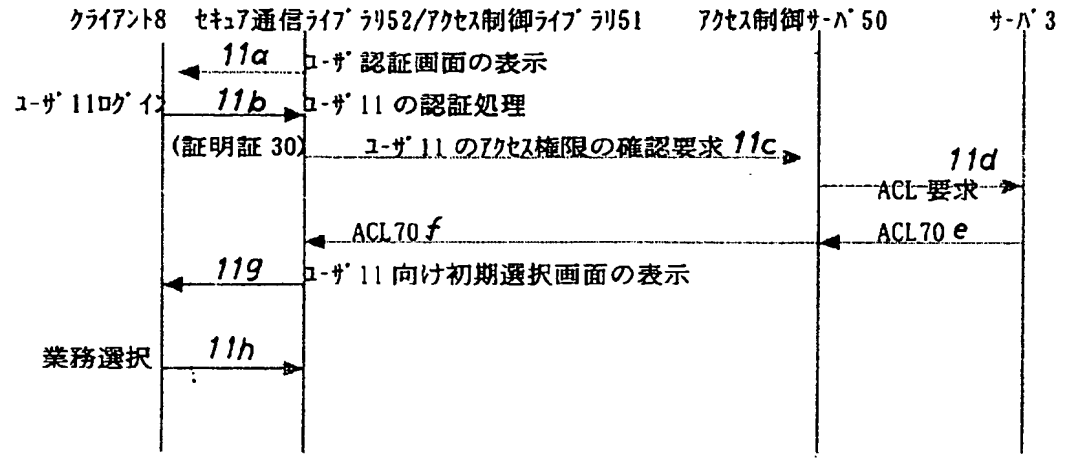
【図１】



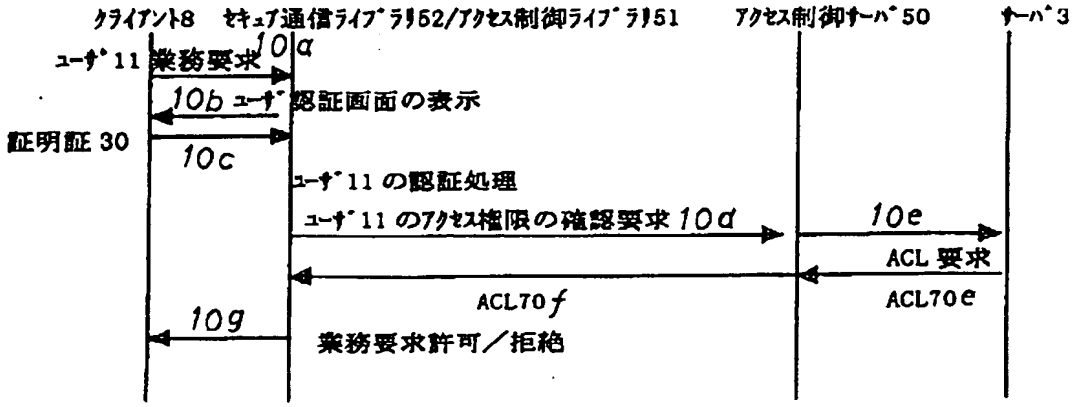
【図2】

ＡＣＬ問合せ手順

(a)



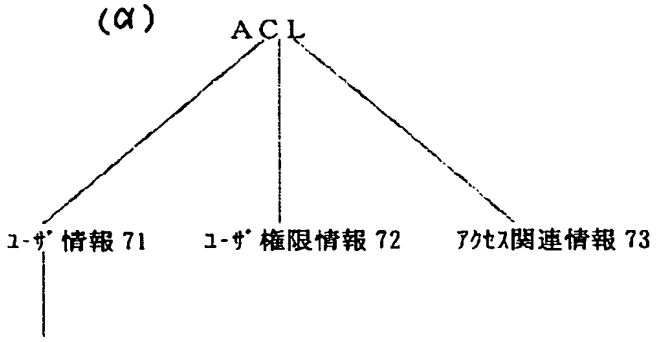
(b)



【図3】

ＡＣＬの一例

(a)



(b) ﾕｰｻﾞ情報 71 の例

ﾕｰｻﾞ識別名称	証明証
ﾕｰｻﾞ 11	証明証 30
ﾕｰｻﾞ 14	証明証 31
...	

(c) その他のﾕｰｻﾞ情報

ﾕｰｻﾞ識別名称	住所	家族構成	入社年度 ...
ﾕｰｻﾞ 11	aaa	bbb	cc

(d) ﾕｰｻﾞ権限情報 72 の事例 1

ﾕｰｻﾞ識別名称	権限ｸﾗｽ
ﾕｰｻﾞ 11	A1
ﾕｰｻﾞ 14	A0

(凡例) 権限ｸﾗｽには A0, A1, A2, A3 を指定。

(e) ﾕｰｻﾞ権限情報 72 の事例 2

ﾕｰｻﾞ識別名称	職制情報
ﾕｰｻﾞ 11	A 部門主任
ﾕｰｻﾞ 14	X 部門ｹﾞｽﾄ

(凡例) 職制情報は部門名称と職位名称 (例:一般、担当、主任、課長、部長等) を指定。

(f) ｱｸｾｽ関連情報 73 の例

権限ｸﾗｽ	ｱｸｾｽ対象	許可内容
A1	業務ｻｰﾊﾞ 6	AP601 起動
	DBｻｰﾊﾞ 5	ﾌｧｲﾙ501 (参照・更新) ﾌｧｲﾙ502 (参照)
	ｸﾞﾙｰﾌﾟｳｪｱ4	制約なし
	接続形態	ﾘﾓｰﾄｱｸｾｽ不可

【図４】

アクセスチケットを用いた制御手順